



Billing Code: 3410-ZV

DEPARTMENT OF AGRICULTURE

Office of the Secretary

Privacy Act of 1974; Revised System of Records

AGENCY: Office of the Chief Information Officer, USDA

ACTION: Notice of the revision of Privacy Act system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Agriculture proposes to revise an existing Department of Agriculture system of records notice now titled, USDA/OCIO-2 eAuthentication Service (eAuth). The USDA eAuth provides the public and government businesses with a single sign-on capability for USDA applications, management of user credentials, and verification of identity, authorization, and electronic signatures. USDA's eAuth collects customer information through an electronic self-registration process provided through the eAuth Web site. This System of Records Notice was previously published as "USDA eAuthentication Service" in Federal Register Vol. 71, No. 143 on Wednesday July 26, 2006. The revision reflects updates to the system name; the system location; routine uses; storage policies; safeguards; retention and disposal; the system manager; and notification, record access, and contesting procedures.

DATES: Submit comments on or before *[INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]*. This new system will be effective *[INSERT DATE 40 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]*.

ADDRESSES: You may submit comments, identified by docket number USDA/OCIO-2 by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: (970) 295-5168
- Mail: Chris North, Enterprise Applications Services Director, eAuthentication, 2150 Centre Avenue, Suite 208, Fort Collins, Colorado 80526
- Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.
- Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Shari Erickson, Program Manager, (970) 295-5128, 301 South Howes Street, Suite 309, Fort Collins, Colorado 80521. For privacy issues, please contact: Ravoyne Payton, Chief Privacy Officer, Technology Planning, Architecture and E-Government, Office of the Chief Information Officer, Department of Agriculture, Washington, D.C. 20250.

SUPPLEMENTARY INFORMATION:

I. Background

The USDA eAuthentication Service provides USDA Agency customers and employees single sign-on capability and electronic authentication and authorization for USDA Web applications and services. Through an online self-registration process, USDA Agency customers and employees can obtain accounts as authorized users that will provide access to USDA resources without needing to re-authenticate within the context of a single

Internet session. Once an account is activated, users may use the associated user ID and password that they created to access USDA resources that are protected by eAuthentication. Information stored in the eAuthentication Service may be shared with other USDA components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies as outlined in the routine uses or authorized by statute. This sharing will take place only after USDA determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice. The revisions to this system of records include renaming the system to be consistent with the Department's naming system; updating the system location, storage policies, storage safeguards, and retention and disposal policies; and the system manager's location; and the notification, record access, and contesting procedures in order to be consistent with the Department's best practices. In addition, the routine uses were amended as follows:

- Former Routine Use 1 was deleted.
- Former Routine Use 2 was renumbered Routine Use 1 and revised.
- Former Routine Use 3 was renumbered Routine Use 2 and revised.
- Former Routine Use 4 was renumbered Routine Use 3 and revised.
- Former Routine Use 5 was renumbered Routine Use 4 and revised.
- Former Routine Use 6 was renumbered Routine Use 5 and revised.
- Routine Use 6 is added to permit disclosure to the Department of Justice in order to represent the government's interest in litigation.

- Routine Use 7 is added to permit disclosure to appropriate agencies, entities, and persons to prevent or address a security breach or suspected security breach.
- Former Routine Use 8 was deleted.

Dated: ____March 6, 2012_____

Thomas J. Vilsack

Secretary

Department of Agriculture

System of Records

USDA/OCIO-2

System name:

USDA/OCIO-2 eAuthentication Service

Security classification:

Unclassified

System location:

USDA-NRCS Information Technology Center, 2150 Centre Avenue Building A,
Fort Collins, Colorado 80526;

USDA-NITC, 8930 Ward Pkwy, Kansas City, Missouri 64114

Categories of individuals covered by the system:

This system contains records on individuals who applied for and were granted
access to USDA applications and services that are protected by eAuthentication.

This includes members of the public and USDA employees.

Categories of records in the system:

Categories of records in this system include:

The eAuthentication system will collect the following information from individuals:

- Name
- Address
- Country of residence
- Telephone number
- Email address
- Date of birth

- Mother's maiden name
- The system will also require users to create a user ID and password

Authority for maintenance of the system:

Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) of 1998; Freedom to E-File Act (Pub. L. 106-222) of 2000; Electronic Signatures in Global and National Commerce Act (E-SIGN, Pub. L. 106-229) of 2000; eGovernment Act of 2002 (H.R. 2458).

Purpose(s):

The records in this system are used to electronically authenticate and authorize users accessing protected USDA applications and services.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Information contained in this system may be disclosed outside USDA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. To external Web applications integrated with the government's federated architecture for authentication. Prior to any disclosure of information under this architecture, the user will request access to an external application with their USDA credential. All external applications will have undergone rigorous testing before joining the architecture. eAuthentication acts as a single sign-on point for USDA Agency applications. This allows a USDA customer to sign onto any USDA applications they have been authorized on via a single sign-on.
2. When a record on its face, on in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in

nature, and whether arising by general statute or particular program, statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate agency, whether Federal, foreign, State, local, tribal, or other public authority responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutive responsibility of the receiving entity.

3. To a court or adjudicative body in a proceeding when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee of the agency in his or her individual capacity where the agency has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.
4. To a congressional office in response to an inquiry made at the written request of the individual to whom the record pertains.
5. At the individual's request to any Federal department, State or local agencies, or USDA partner utilizing or interfacing with eAuthentication to provide electronic authentication for electronic transactions. The disclosure of this information is required to securely provide, monitor, and analyze the requested program, service, registration, or other transaction.

6. To the Department of Justice when: (a) the agency or any component thereof; or (b) any employee of the agency in his or her official capacity; or (c) any employee in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.
7. To appropriate agencies, entities, and persons when (1) USDA suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the USDA has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the USDA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the USDA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure to consumer reporting agencies:

None.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Records are stored and maintained electronically on USDA-owned and operated systems in Kansas City, Missouri and Fort Collins, Colorado.

Retrievability:

Records can be retrieved by name, username, or system ID.

Safeguards:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable USDA automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

Retention and disposal:

Records in this system will be retained in accordance with approved retention schedules, including: (1) Audit Reports File (N1-485-08-2, item 17), which provides for annual cut-off and for destruction 10 years after cutoff; and (2) Audit Work papers (N1-485- 08-2, item 2), which provides for annual cut-off and for destruction 6 years and 3 months after cut-off. Additional approved schedules may apply. Destruction of records shall occur in the manner(s) appropriate to the type of record, such as shredding of paper records and/or deletion of computer records.

System Manager and address:

Program Manager - Identity and Access Management, 301 South Howes Street Suite 309,
Fort Collins, Colorado 80521

Notification procedure:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component's FOIA Officer, whose contact information can be found at <http://www.dm.usda.gov/foia.htm> under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief FOIA Officer, Department of Agriculture, 1400 Independence Avenue, S.W., Washington, D.C. 20250.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief FOIA Officer, Department of Agriculture, 1400 Independence Avenue, S.W., Washington, D.C. 20250. In addition, you should provide the following:

- An explanation of why you believe the Department would have information on you,

- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which USDA component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information, the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

Record access procedures:

See “Notification procedure” above.

Contesting record procedures:

See “Notification procedure” above.

Record source categories:

Information from the system will be submitted by the user. When a user wishes to transact with USDA or its partner organizations electronically, the user must enter name, address, country of residence, telephone number, date of birth, mother’s maiden name, username, and password. As the USDA eAuthentication Service is integrated with other government or private sector authentication systems, data may be obtained from those systems to facilitate single-sign on capabilities with the user’s permission.

Exemptions claimed for the system: None.

U.S. Department of Agriculture
Narrative Statement on revised eAuthentication
System of Records under the Privacy Act of 1974
USDA/OCIO-2 eAuthentication Service

The U.S. Department of Agriculture (USDA) eAuthentication Service provides USDA Agency customers and employees single sign-on capability and electronic authentication and authorization for USDA Web applications and services. Through an online self-registration process, USDA Agency customers and employees can obtain accounts as authorized users that will provide access to USDA resources without needing to re-authenticate within the context of a single Internet session. Once an account is activated, users may use the associated user ID and password that they created to access USDA resources that are protected by eAuthentication. Information stored in the eAuthentication Service may be shared with other USDA components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies as outlined in the routine uses or authorized by statute. This sharing will take place only after USDA determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice. USDA is publishing the routine uses pursuant to which it may disclose information about individuals to the extent the disclosure is consistent with the purpose for which the information was collected. Routine uses include disclosure to external Web applications upon user request, to other government agencies for law enforcement purposes if the record on its face or in conjunction with other records indicates a violation of law, to a

court or adjudicative body if relevant and necessary to appropriate litigation, to a congressional office upon written request of the individual, to other government entities of USDA partners upon user request, to USDA contractors or industry to identify fraud, waste, or abuse to the Department of Justice if relevant and necessary for appropriate litigation, or to agencies, entities, or persons to prevent or remedy security breach.

The authority for maintaining this system is derived from: Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) of 1998; Freedom to E-File Act (Pub. L. 106-222) of 2000; Electronic Signatures in Global and National Commerce Act (E-SIGN, Pub. L. 106-229) of 2000; eGovernment Act of 2002 (H.R. 2458).

Probable or potential effects on the privacy of individuals:

Although there is some risk to the privacy of individuals, that risk is outweighed by the benefits to those individuals who will be able to access multiple programs and applications with a single login. In addition, the safeguards in place will protect against unauthorized disclosure. Records are accessible only to individuals who are authorized, and physical and electronic safeguards are employed to ensure security.

eAuthentication has a current Authority to Operate obtained via the completion of a Cyber Security Certification and Accreditation (C&A). A satisfactory risk assessment has been performed.

OMB information collection requirements:

OMB information collection approval: OMB No. 0503-0014

